FIG. 1

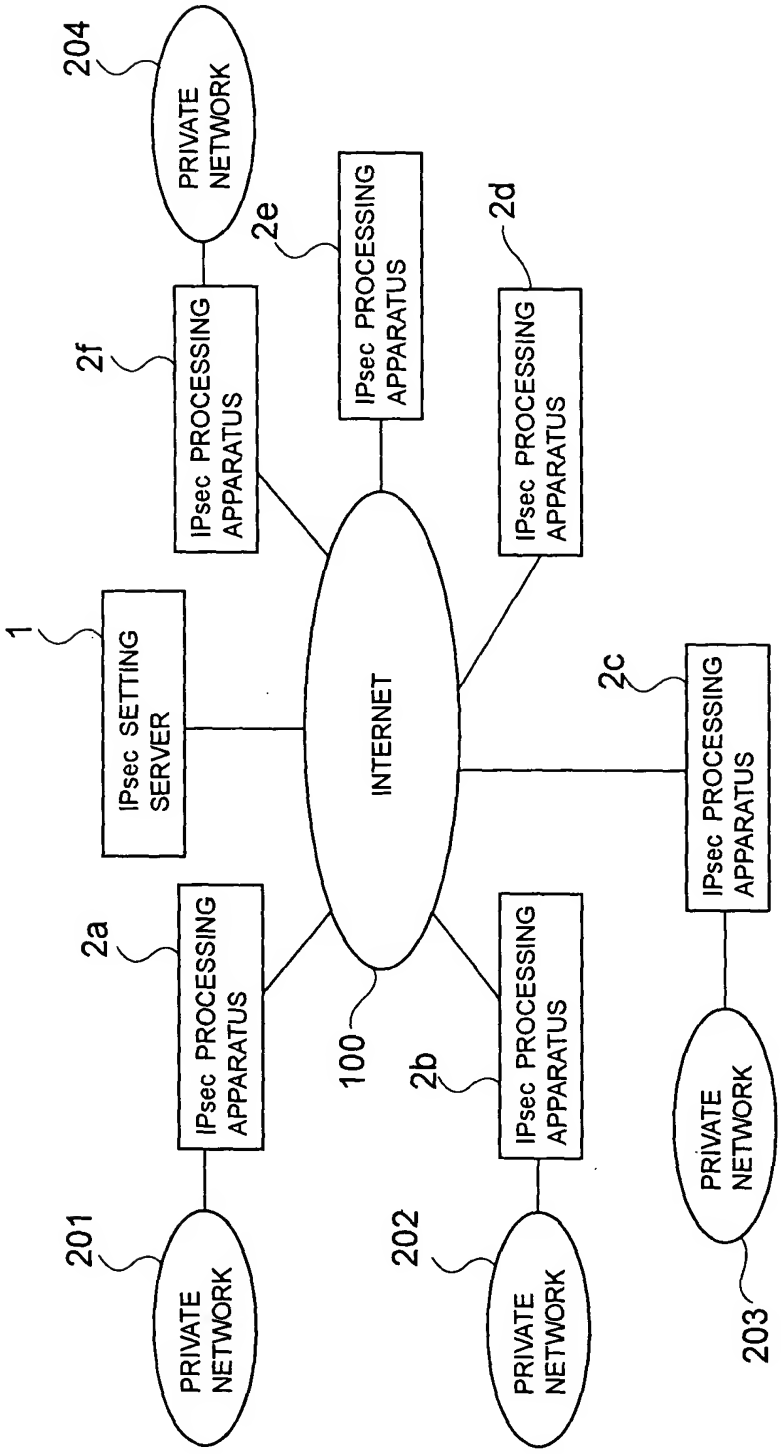
204
PRIVATE NETWORK
2e
IPsec PROCESSING APPARATUS
2d
IPsec PROCESSING APPARATUS
2f
IPsec PROCESSING APPARATUS
1
IPsec SETTING SERVER
INTERNET
2c
IPsec PROCESSING APPARATUS
2a
IPsec PROCESSING APPARATUS
100
2b
IPsec PROCESSING APPARATUS
PRIVATE NETWORK
201
PRIVATE NETWORK
202
PRIVATE NETWORK
203

FIG. 2

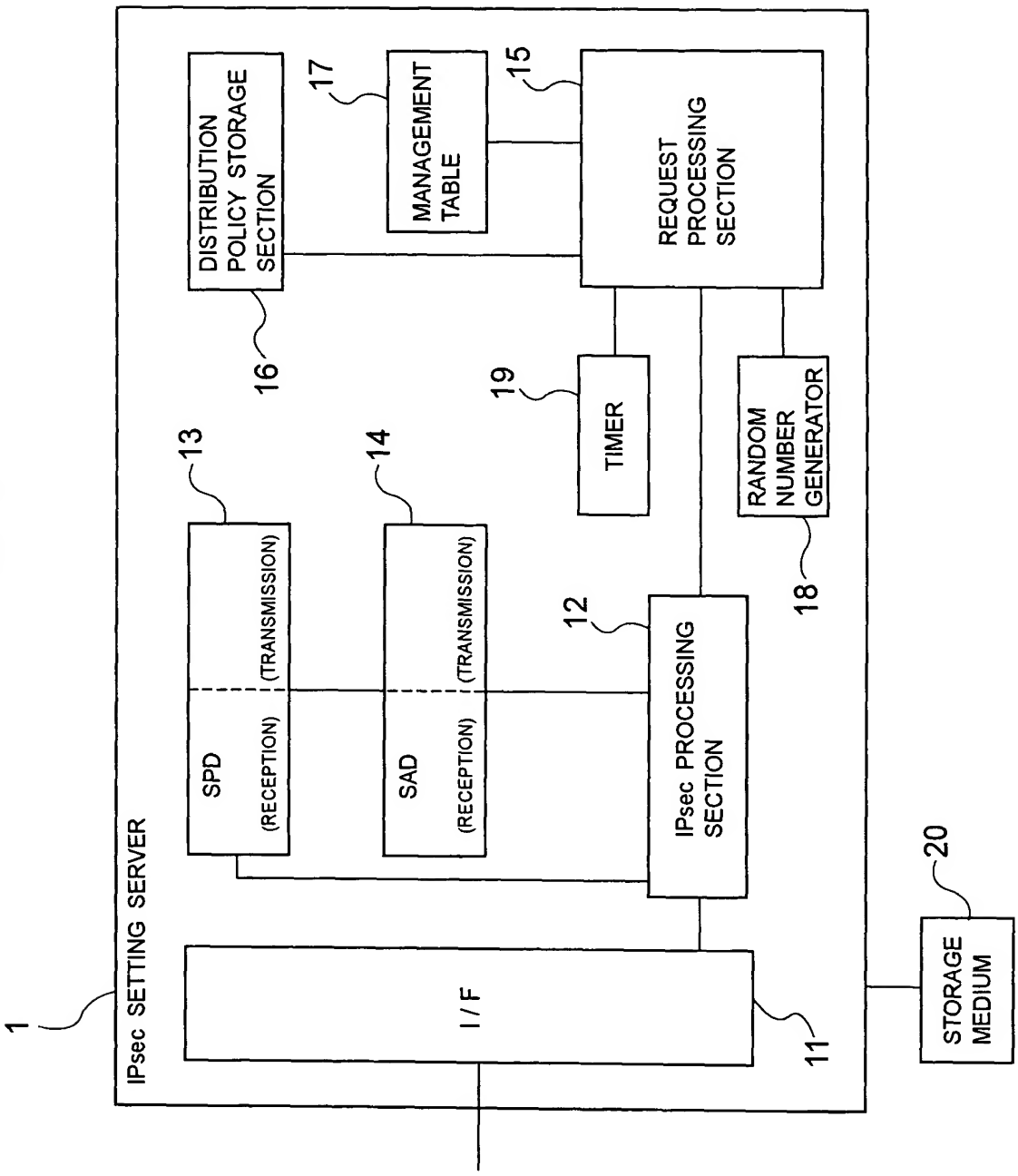
1
IPsec SETTING SERVER
I / F
11
SPD
(RECEPTION)
(TRANSMISSION)
13
SAD
(RECEPTION)
(TRANSMISSION)
14
IPsec PROCESSING SECTION
12
DISTRIBUTION POLICY STORAGE SECTION
16
MANAGEMENT TABLE
17
REQUEST PROCESSING SECTION
15
TIMER
19
RANDOM NUMBER GENERATOR
18
STORAGE MEDIUM
20

FIG. 3

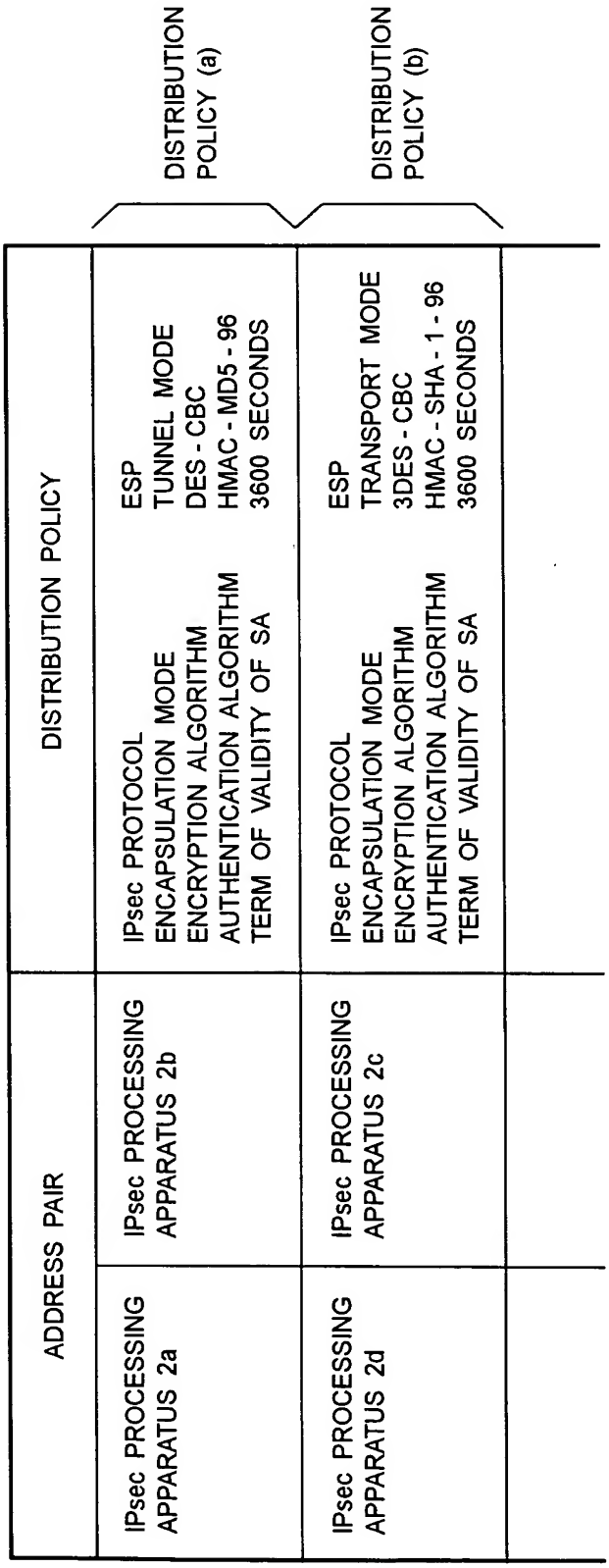
ADDRESS PAIR
DISTRIBUTION POLICY
IPsec PROCESSING APPARATUS 2a
IPsec PROCESSING APPARATUS 2b
IPsec PROCESSING APPARATUS 2c
IPsec PROCESSING APPARATUS 2d
IPsec PROTOCOL ESP
ENCAPSULATION MODE TUNNEL MODE
ENCRYPTION ALGORITHM DES - CBC
AUTHENTICATION ALGORITHM HMAC - MD5 - 96
TERM OF VALIDITY OF SA 3600 SECONDS
DISTRIBUTION POLICY (a)
IPsec PROTOCOL ESP
ENCAPSULATION MODE TRANSPORT MODE
ENCRYPTION ALGORITHM 3DES - CBC
AUTHENTICATION ALGORITHM HMAC - SHA - 1 - 96
TERM OF VALIDITY OF SA 3600 SECONDS
DISTRIBUTION POLICY (b)

FIG. 4

ID	REQUEST SOURCE ADDRESS	OPPOSITE PARTY ADDRESS	REQUEST ID	SPI	SETTING PARAMETERS
1	IPsec PROCESSING APPARATUS 2a	IPsec PROCESSING APPARATUS 2b	1001	5100	APPLICATION POLICY DISTRIBUTION POLICY (a) SA PARAMETER FOR 2a → 2b SA PARAMETER (a) SA PARAMETER FOR 2b → 2a SA PARAMETER (b)
	IPsec PROCESSING APPARATUS 2b	IPsec PROCESSING APPARATUS 2a	2001	6100	
2	IPsec PROCESSING APPARATUS 2a	IPsec PROCESSING APPARATUS 2b	1002	5110	APPLICATION POLICY DISTRIBUTION POLICY (a) SA PARAMETER FOR 2a → 2b SA PARAMETER FOR 2b → 2a
	IPsec PROCESSING APPARATUS 2b	IPsec PROCESSING APPARATUS 2a			
3					

FIG. 5

IPsec PROTOCOL	ESP
ENCAPSULATION MODE	TUNNEL MODE
ENCRYPTION ALGORITHM	DES - CBC
AUTHENTICATION ALGORITHM	HMAC - MD5 - 96
TERM OF VALIDITY	3600 SECONDS
ENCRYPTION KEY	0x7d5e837ad . . .
AUTHENTICATION KEY	0x89e562bfc . . .
IV	0xc32fbe004 . . .
RECEPTION SIDE SPI	6100

FIG. 6

MESSAGE TYPE	REQUEST MESSAGE
ID	1001
REQUEST SOURCE ADDRESS	IPsec PROCESSING APPARATUS 2a
OPPOSITE PARTY ADDRESS	IPsec PROCESSING APPARATUS 2b
SPI	5100

FIG. 7

MESSAGE TYPE	DISTRIBUTION MESSAGE
ID	1001
REQUEST SOURCE ADDRESS	IPsec PROCESSING APPARATUS 2a
OPPOSITE PARTY ADDRESS	IPsec PROCESSING APPARATUS 2b
SETTING PARAMETER	
OPERATION POLICY	DISTRIBUTION POLICY (a)
SA PARAMETER FOR 2a → 2b	SA PARAMETER (a)
SA PARAMETER FOR 2b → 2a	SA PARAMETER (b)

FIG. 8

MESSAGE TYPE	REQUEST STARTUP MESSAGE
OPPOSITE PARTY ADDRESS	IPsec PROCESSING APPARATUS 2a

FIG. 9

MESSAGE TYPE	NO CORRESPONDING ENTRY ERROR MESSAGE
ID	1001
REQUEST SOURCE ADDRESS	IPsec PROCESSING APPARATUS 2a
OPPOSITE PARTY ADDRESS	IPsec PROCESSING APPARATUS 2b

FIG. 10

MESSAGE TYPE	CONTENT INCONSISTENCY ERROR MESSAGE	
ID	1001	
REQUEST SOURCE ADDRESS	IPsec PROCESSING APPARATUS 2a	
OPPOSITE PARTY ADDRESS	IPsec PROCESSING APPARATUS 2b	
ENTRY LIST	ID	SPI
	1001	5100
	1002	5110

FIG. 11

MESSAGE TYPE	NO - RESPONSE ERROR MESSAGE
ID	1001
REQUEST SOURCE ADDRESS	IPsec PROCESSING APPARATUS 2a
OPPOSITE PARTY ADDRESS	IPsec PROCESSING APPARATUS 2b

FIG. 12

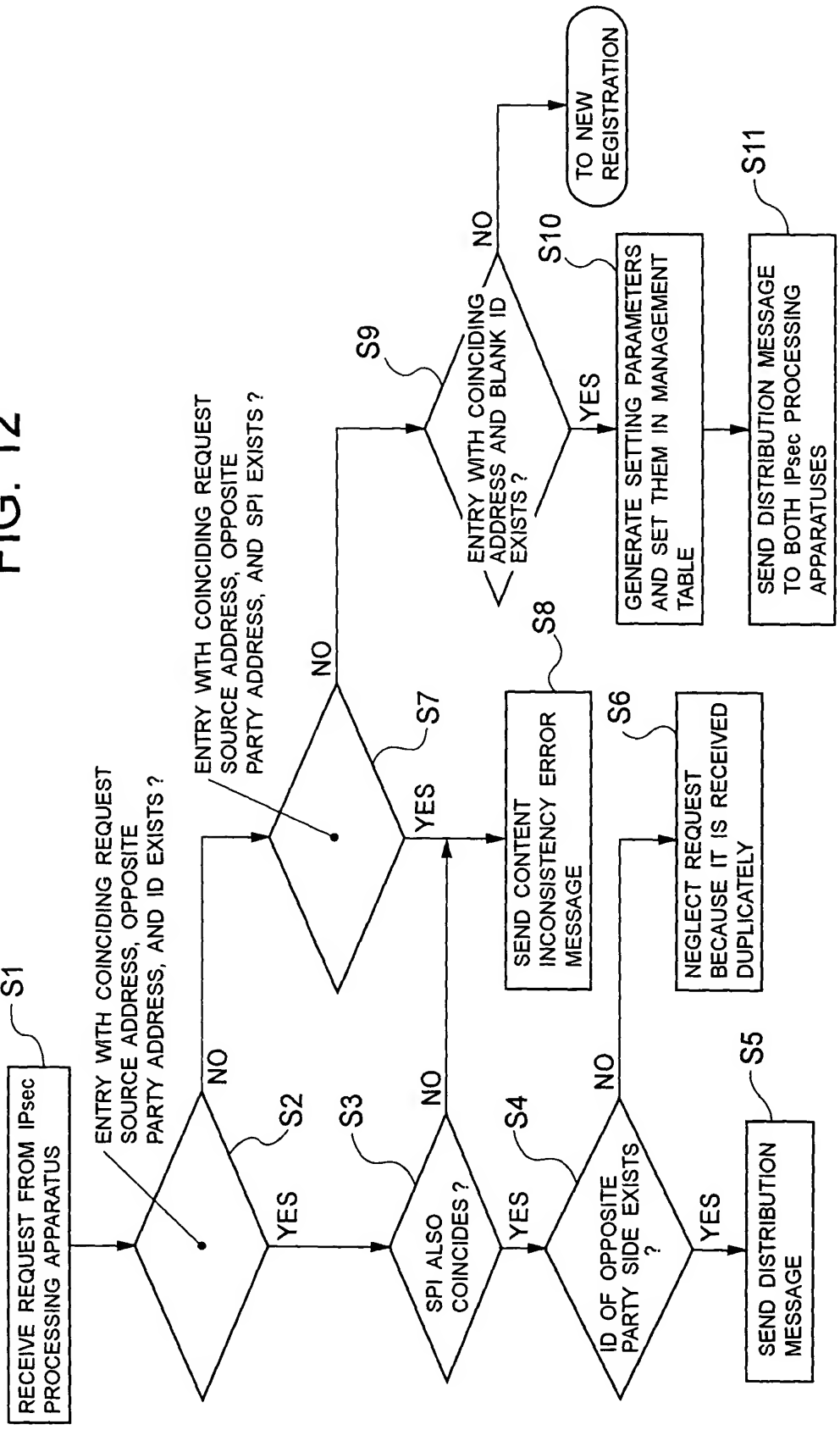
S1
RECEIVE REQUEST FROM IPsec PROCESSING APPARATUS
ENTRY WITH COINCIDING REQUEST SOURCE ADDRESS, OPPOSITE PARTY ADDRESS, AND ID EXISTS ?
NO
YES
S2
S3
SPI ALSO COINCIDES ?
NO
YES
S4
ID OF OPPOSITE PARTY SIDE EXISTS ?
NO
YES
S5
SEND DISTRIBUTION MESSAGE
S6
NEGLECT REQUEST BECAUSE IT IS RECEIVED DUPLICATELY
ENTRY WTH COINCIDING REQUEST SOURCE ADDRESS, OPPOSITE PARTY ADDRESS, AND SPI EXISTS ?
NO
YES
S7
SEND CONTENT INCONSISTENCY ERROR MESSAGE
S8
ENTRY WITH COINCIDING ADDRESS AND BLANK ID EXISTS ?
NO
YES
S9
TO NEW REGISTRATION
GENERATE SETTING PARAMETERS AND SET THEM IN MANAGEMENT TABLE
S10
SEND DISTRIBUTION MESSAGE TO BOTH IPsec PROCESSING APPARATUSES
S11

FIG.13

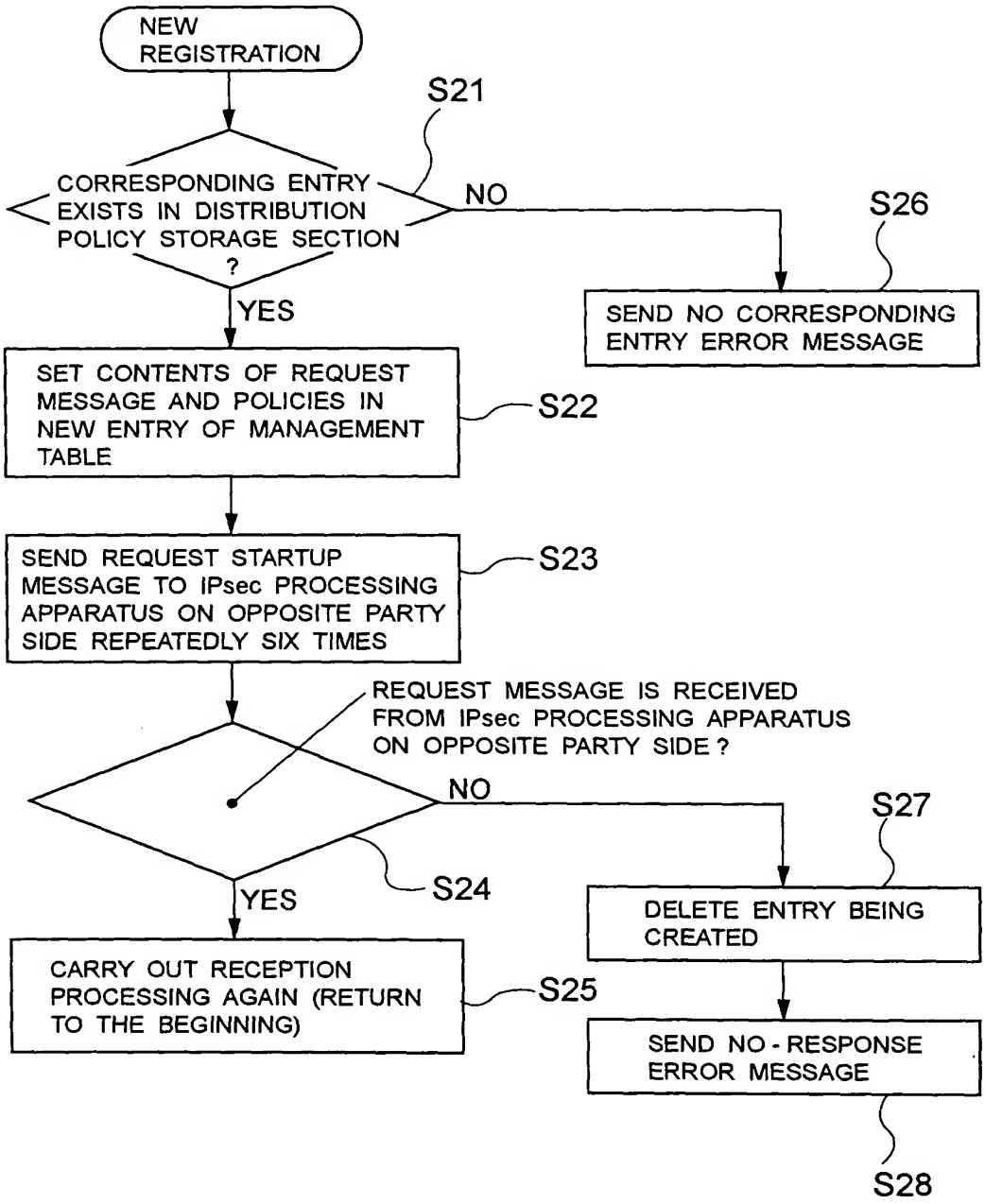
NEW REGISTRATION
S21
CORRESPONDING ENTRY EXISTS IN DISTRIBUTION POLICY STORAGE SECTION ?
NO
S26
SEND NO CORRESPONDING ENTRY ERROR MESSAGE
YES
SET CONTENTS OF REQUEST MESSAGE AND POLICIES IN NEW ENTRY OF MANAGEMENT TABLE
S22
SEND REQUEST STARTUP MESSAGE TO IPsec PROCESSING APPARATUS ON OPPOSITE PARTY SIDE REPEATEDLY SIX TIMES
S23
REQUEST MESSAGE IS RECEIVED FROM IPsec PROCESSING APPARATUS ON OPPOSITE PARTY SIDE ?
NO
S27
S24
YES
DELETE ENTRY BEING CREATED
CARRY OUT RECEPTION PROCESSING AGAIN (RETURN TO THE BEGINNING)
S25
SEND NO - RESPONSE ERROR MESSAGE
S28

FIG. 14

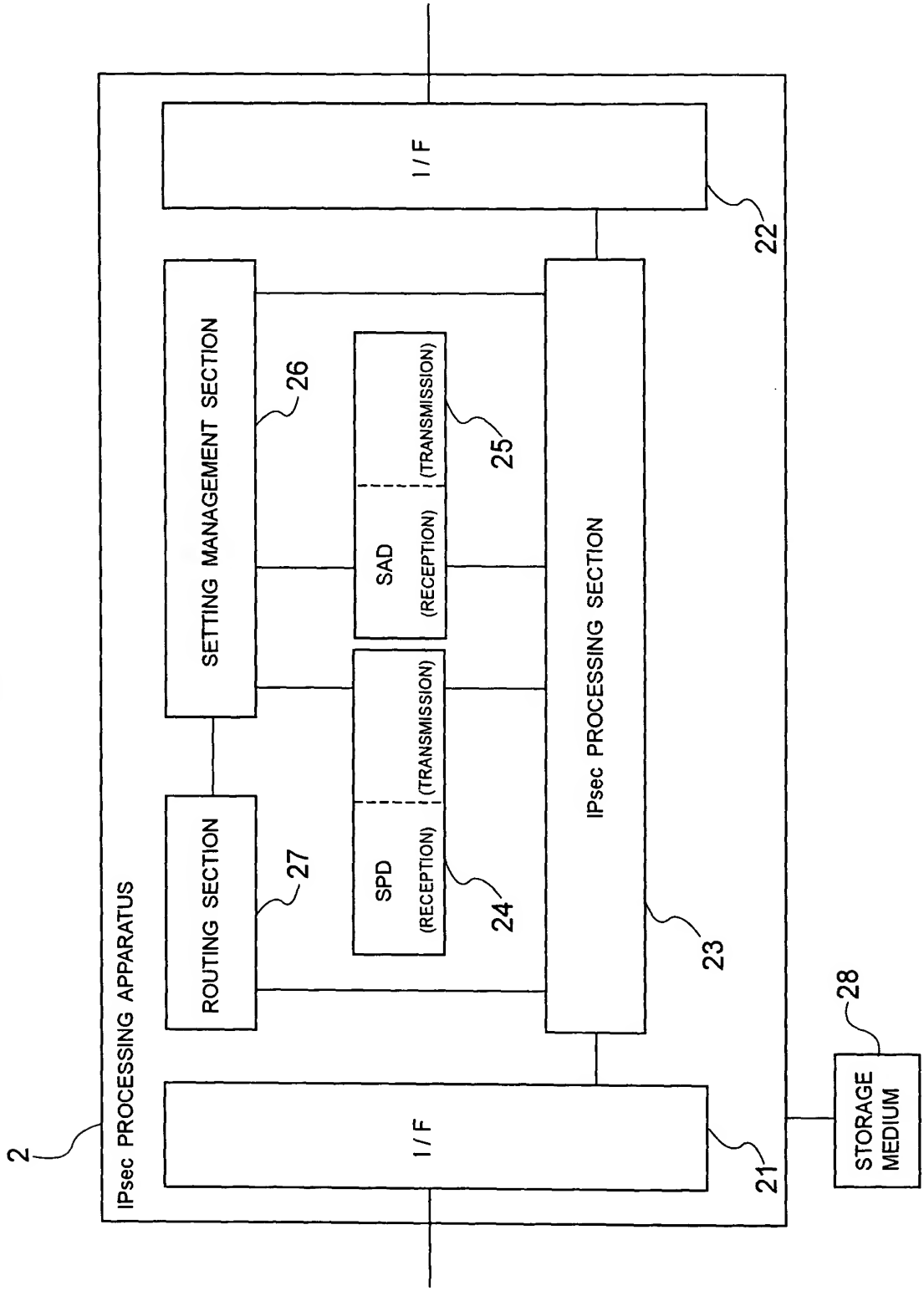
IPsec PROCESSING APPARATUS
2
I / F
22
SETTING MANAGEMENT SECTION
26
SAD
(RECEPTION)
(TRANSMISSION)
25
SPD
(RECEPTION)
(TRANSMISSION)
24
ROUTING SECTION
27
IPsec PROCESSING SECTION
23
I / F
21
STORAGE MEDIUM
28

FIG. 15

ID	SELECTOR	PROCESS	IPsec APPLICATION POLICY	OPPOSITE PARTY ADDRESS FOR SETTING REQUEST
1	APPARATUS OF ITS OWN → SETTING SERVER 1	IPsec	APPLICATION POLICY (z)	
2	TO PRIVATE NETWORK 202	IPsec		IPsec PROCESSING APPARATUS 2b
3	TO PRIVATE NETWORK 203	IPsec		IPsec PROCESSING APPARATUS 2c
4	ALL OTHER THAN THE ABOVE	PASS		

FIG. 16

IPsec APPLICATION POLICY	
IPsec PROTOCOL	ESP
ENCAPSULATION MODE	TRANSPORT MODE
OPPOSITE PARTY ADDRESS	SETTING SERVER 1
ENCRYPTION ALGORITHM	AES - CBC
AUTHENTICATION ALGORITHM	HMAC - SHA - 1 - 96
TERM OF VALIDITY OF SA	3600 SECONDS
IKE POLICY	
OPPOSITE PARTY IPsec PROCESSING APPARATUS ADDRESS	SETTING SERVER 1
OPPOSITE PARTY AUTHENTICATION SYSTEM	PRIOR COMMON SECRET KEY
PRIOR COMMON SECRET KEY	password - for - ike
ENCRYPTION ALGORITHM	DES - CBC
HASH ALGORITHM	MD5
Oakley GROUP	1536 BIT MODP GROUP
TERM OF VALIDITY OF SA	3600 SECONDS

FIG. 17

ID	KEY PARAMETERS			SA PARAMETERS	
	TERMINAL ADDRESS	IPsec	SPI		
1	IPsec PROCESSING APPARATUS 2b	ESP	6100	ENCAPSULATION MODE	TUNNEL MODE
				ENCRYPTION ALGORITHM	DES - CBC
				AUTHENTICATION ALGORITHM	HMAC - MD5 - 96
				ENCRYPTION KEY	0x7d5e837ad...
				AUTHENTICATION KEY	0x83e562bfc...
				IV	0xc32fbe004...
				TERM OF VALIDITY	3600 SECONDS
				SEQUENCE NUMBER	0
2	SETTING SERVER 1	ESP	6100	ENCAPSULATION MODE	TRANSPORT MODE
				ENCRYPTION ALGORITHM	AES - CBC
				AUTHENTICATION ALGORITHM	HMAC - SHA - 96
				ENCRYPTION KEY	0xda738e5d7...
				AUTHENTICATION KEY	0xcfb265c98...
				IV	0xc399ebf22...
				TERM OF VALIDITY	3600 SECONDS
				SEQUENCE NUMBER	2133
3					

FIG.18

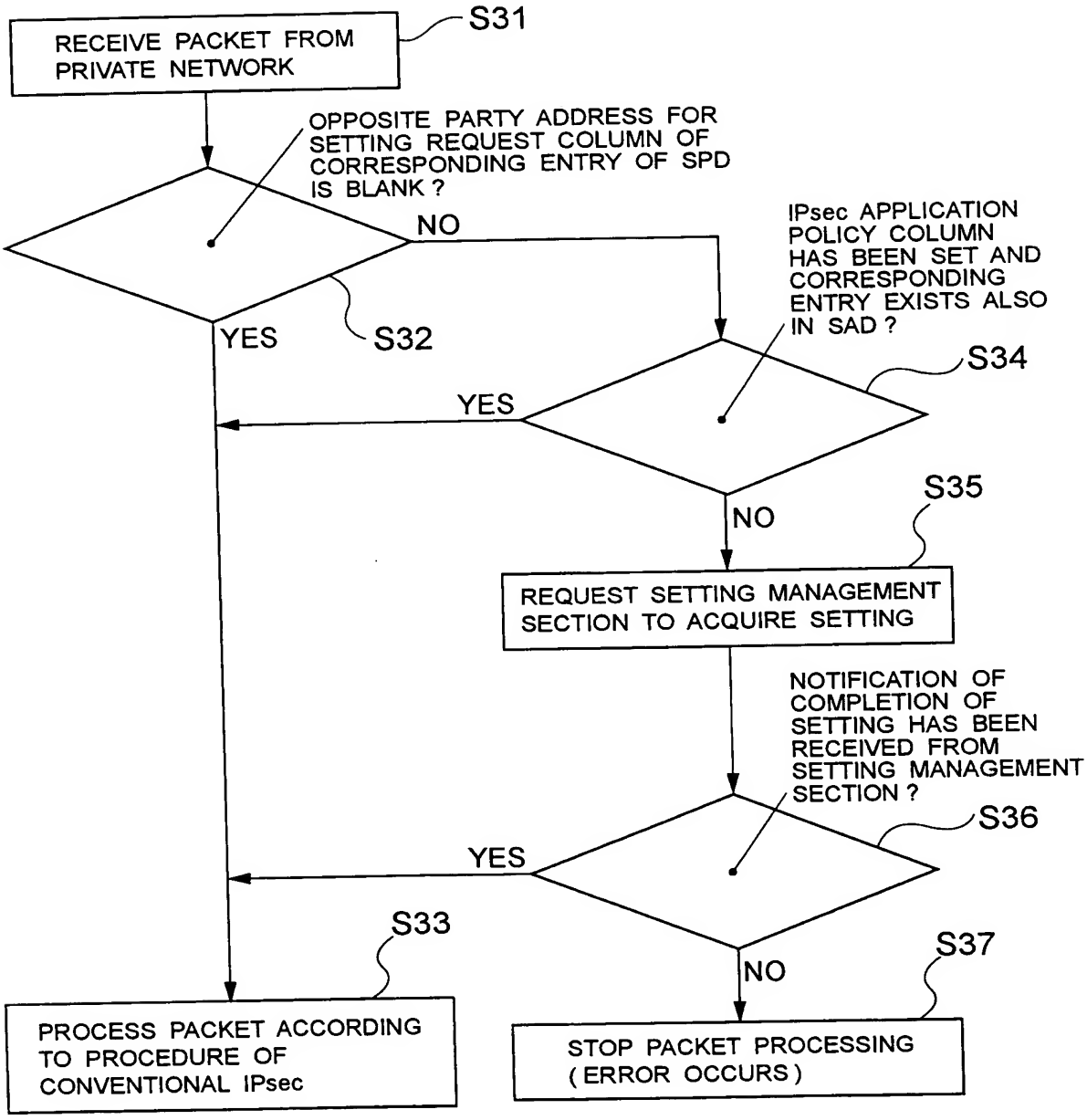
RECEIVE PACKET FROM PRIVATE NETWORK
S31
OPPOSITE PARTY ADDRESS FOR SETTING REQUEST COLUMN OF CORRESPONDING ENTRY OF SPD IS BLANK ?
NO
YES
S32
IPsec APPLICATION POLICY COLUMN HAS BEEN SET AND CORRESPONDING ENTRY EXISTS ALSO IN SAD ?
S34
YES
NO
S35
REQUEST SETTING MANAGEMENT SECTION TO ACQUIRE SETTING
NOTIFICATION OF COMPLETION OF SETTING HAS BEEN RECEIVED FROM SETTING MANAGEMENT SECTION ?
S36
YES
NO
S37
S33
PROCESS PACKET ACCORDING TO PROCEDURE OF CONVENTIONAL IPsec
STOP PACKET PROCESSING (ERROR OCCURS)

FIG. 19

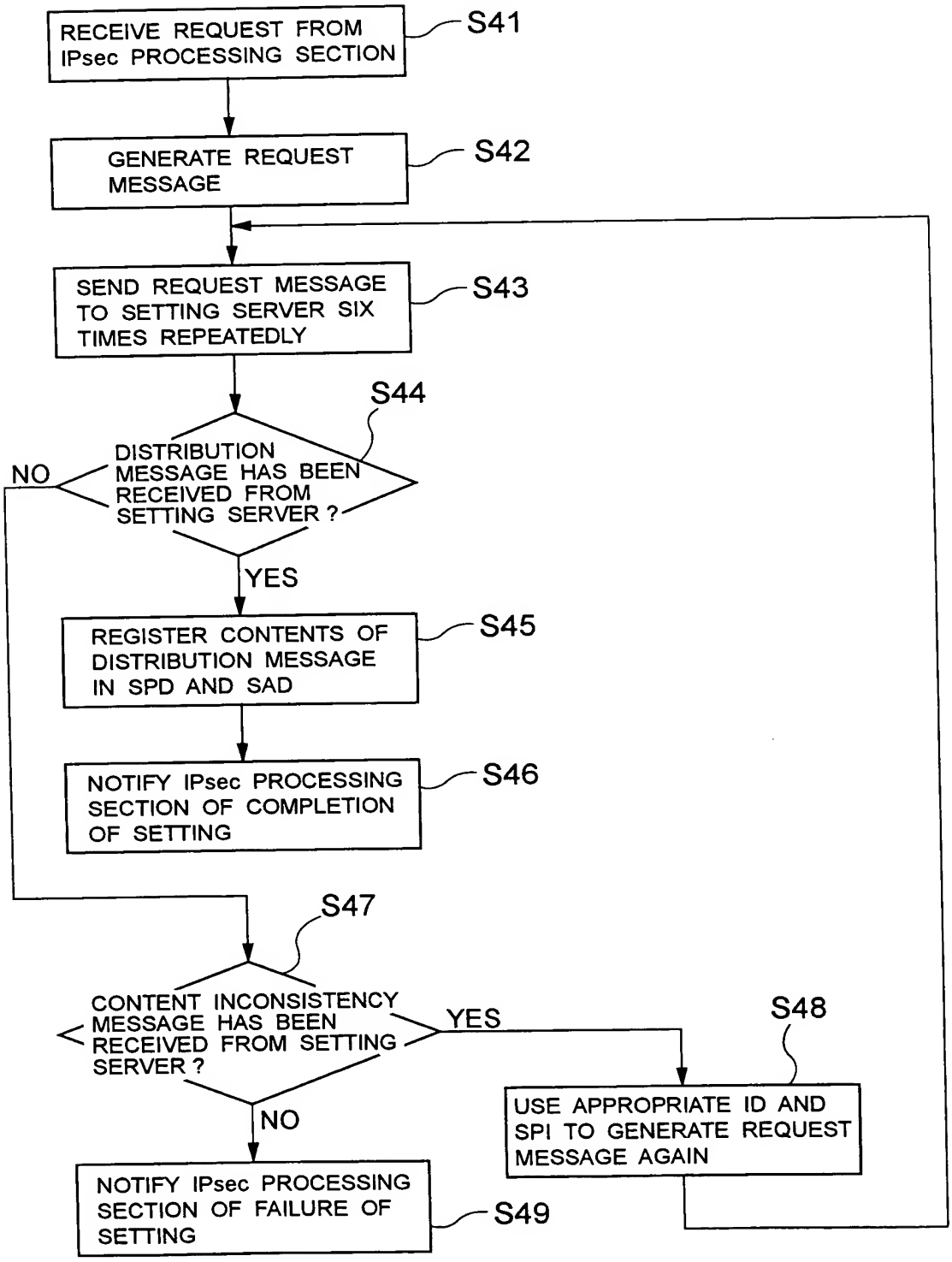
RECEIVE REQUEST FROM IPsec PROCESSING SECTION
S41
GENERATE REQUEST MESSAGE
S42
SEND REQUEST MESSAGE TO SETTING SERVER SIX TIMES REPEATEDLY
S43
S44
DISTRIBUTION MESSAGE HAS BEEN RECEIVED FROM SETTING SERVER ?
NO
YES
REGISTER CONTENTS OF DISTRIBUTION MESSAGE IN SPD AND SAD
S45
NOTIFY IPsec PROCESSING SECTION OF COMPLETION OF SETTING
S46
S47
CONTENT INCONSISTENCY MESSAGE HAS BEEN RECEIVED FROM SETTING SERVER ?
YES
S48
NO
USE APPROPRIATE ID AND SPI TO GENERATE REQUEST MESSAGE AGAIN
NOTIFY IPsec PROCESSING SECTION OF FAILURE OF SETTING
S49

FIG. 20

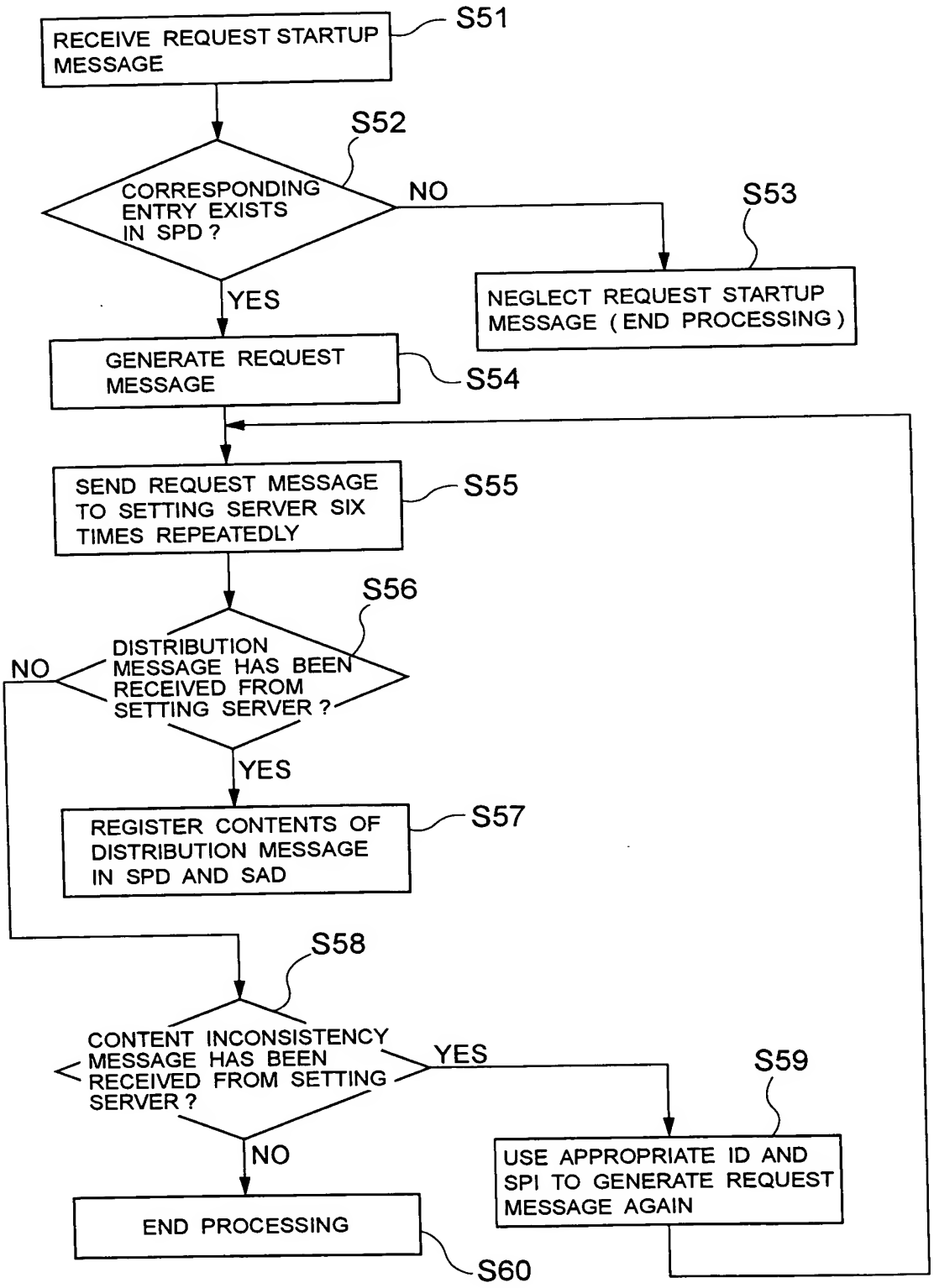
RECEIVE REQUEST STARTUP MESSAGE
S51
CORRESPONDING ENTRY EXISTS IN SPD ?
S52
NO
S53
NEGLECT REQUEST STARTUP MESSAGE (END PROCESSING)
YES
GENERATE REQUEST MESSAGE
S54
SEND REQUEST MESSAGE TO SETTING SERVER SIX TIMES REPEATEDLY
S55
DISTRIBUTION MESSAGE HAS BEEN RECEIVED FROM SETTING SERVER ?
S56
NO
YES
REGISTER CONTENTS OF DISTRIBUTION MESSAGE IN SPD AND SAD
S57
CONTENT INCONSISTENCY MESSAGE HAS BEEN RECEIVED FROM SETTING SERVER ?
S58
YES
S59
NO
USE APPROPRIATE ID AND SPI TO GENERATE REQUEST MESSAGE AGAIN
END PROCESSING
S60

FIG. 21

ID	SELECTOR	PROCESSING	IPsec APPLICATION POLICY
1	IPsec SETTING SERVER 1 → IPsec PROCESSING APPARATUS 2a	IPsec	APPLICATION POLICY (v)
2	IPsec SETTING SERVER 1 → IPsec PROCESSING APPARATUS 2b	IPsec	APPLICATION POLICY (w)
3	IPsec SETTING SERVER 1 → IPsec PROCESSING APPARATUS 2c	IPsec	APPLICATION POLICY (x)
4	IPsec SETTING SERVER 1 → IPsec PROCESSING APPARATUS 2d	IPsec	APPLICATION POLICY (y)
5	ALL OTHER THAN THE ABOVE	DISPOSAL	

FIG. 22

IPsec APPLICATION POLICY	
IPsec PROTOCOL	ESP
ENCAPSULATION MODE	TRANSPORT MODE
OPPOSITE PARTY ADDRESS	IPsec PROCESSING APPARATUS 2a
ENCRYPTION ALGORITHM	AES - CBC
AUTHENTICATION ALGORITHM	HMAC - SHA - 1 - 96
TERM OF VALIDITY OF SA	3600 SECONDS
IKE POLICY	
OPPOSITE PARTY IPsec PROCESSING APPARATUS ADDRESS	IPsec PROCESSING APPARATUS 2A
OPPOSITE PARTY RECOGNITION SYSTEM	PRIOR COMMON SECRET KEY
PRIOR COMMON SECRET KEY	password - for - ike
ENCRYPTION ALGORITHM	DES - CBC
HASH ALGORITHM	MD5
Oakley GROUP	1536 BIT MODP GROUP
TERM OF VALIDITY OF SA	3600 SECONDS

FIG. 23

ID	SELECTOR	PROCESSING	IPsec APPLICATION POLICY
1	TO PRIVATE NETWORK 202	IPsec	APPLICATION POLICY (j)
2	TO PRIVATE NETWORK 203	IPsec	APPLICATION POLICY (k)
3	ALL OTHER THAN THE ABOVE	PASS	

FIG. 24

IPsec APPLICATION POLICY	
IPsec PROTOCOL	ESP
ENCAPSULATION MODE	TUNNEL MODE
OPPOSITE PARTY ADDRESS	IPsec PROCESSING APPARATUS 2b
ENCRYPTION ALGORITHM	AES - CBC
AUTHENTICATION ALGORITHM	HMAC - MD5 - 96
TERM OF VALIDITY OF SA	3600 SECONDS
IKE POLICY	
OPPOSITE PARTY IPsec PROCESSING APPARATUS ADDRESS	IPsec PROCESSING APPARATUS 2b
OPPOSITE PARTY AUTHENTICATION SYSTEM	PRIOR COMMON SECRET KEY
PRIOR COMMON SECRET KEY	password
ENCRYPTION ALGORITHM	DES - CBC
HASH ALGORITHM	MD5
Oakley GROUP	1536 BIT MODP GROUP
TERM OF VALIDITY OF SA	3600 SECONDS

FIG. 25

ID	REQUEST SOURCE ADDRESS	OPPOSITE PARTY ADDRESS	REQUEST ID	SPI	SETTING PARAMETERS
1	IPsec PROCESSING APPARATUS 2a	IPsec PROCESSING APPARATUS 2b	1001	5100	APPLICATION POLICY DISTRIBUTION POLICY (a) SA PARAMETER FOR 2a → 2b SA PARAMETER FOR 2b → 2a
	IPsec PROCESSING APPARATUS 2b	IPsec PROCESSING APPARATUS 2a			
2					APPLICATION POLICY
3					

FIG. 26

ID	SELECTOR	PROCESSING	IPsec APPLICATION POLICY	OPPOSITE PARTY ADDRESS FOR SETTING REQUEST
1	APPARATUS OF ITS OWN → SETTING SERVER 1	IPsec	APPLICATION POLICY (z)	
2	TO PRIVATE NETWORK 202	IPsec	APPLICATION POLICY (a)	IPsec PROCESSING APPARATUS 2b
3	TO PRIVATE NETWORK 203	IPsec		IPsec PROCESSING APPARATUS 2c
4	ALL OTHER THAN THE ABOVE	PASS		

FIG. 27

ID	REQUEST SOURCE ADDRESS	OPPOSITE PARTY ADDRESS	REQUEST ID	SPI	SETTING PARAMETERS
1	IPsec PROCESSING APPARATUS 2a	IPsec PROCESSING APPARATUS 2b	1001	5100	APPLICATION POLICY DISTRIBUTION POLICY (a) SA PARAMETER FOR 2a → 2b SA PARAMETER (a) SA PARAMETER FOR 2b → 2a SA PARAMETER (b)
	IPsec PROCESSING APPARATUS 2b	IPsec PROCESSING APPARATUS 2a	2001	6100	
2	IPsec PROCESSING APPARATUS 2a	IPsec PROCESSING APPARATUS 2b	1002	5110	APPLICATION POLICY DISTRIBUTION POLICY (a) SA PARAMETER FOR 2a → 2b SA PARAMETER (c) SA PARAMETER FOR 2b → 2a SA PARAMETER (d)
	IPsec PROCESSING APPARATUS 2b	IPsec PROCESSING APPARATUS 2a	2002	6110	
3					

FIG. 28

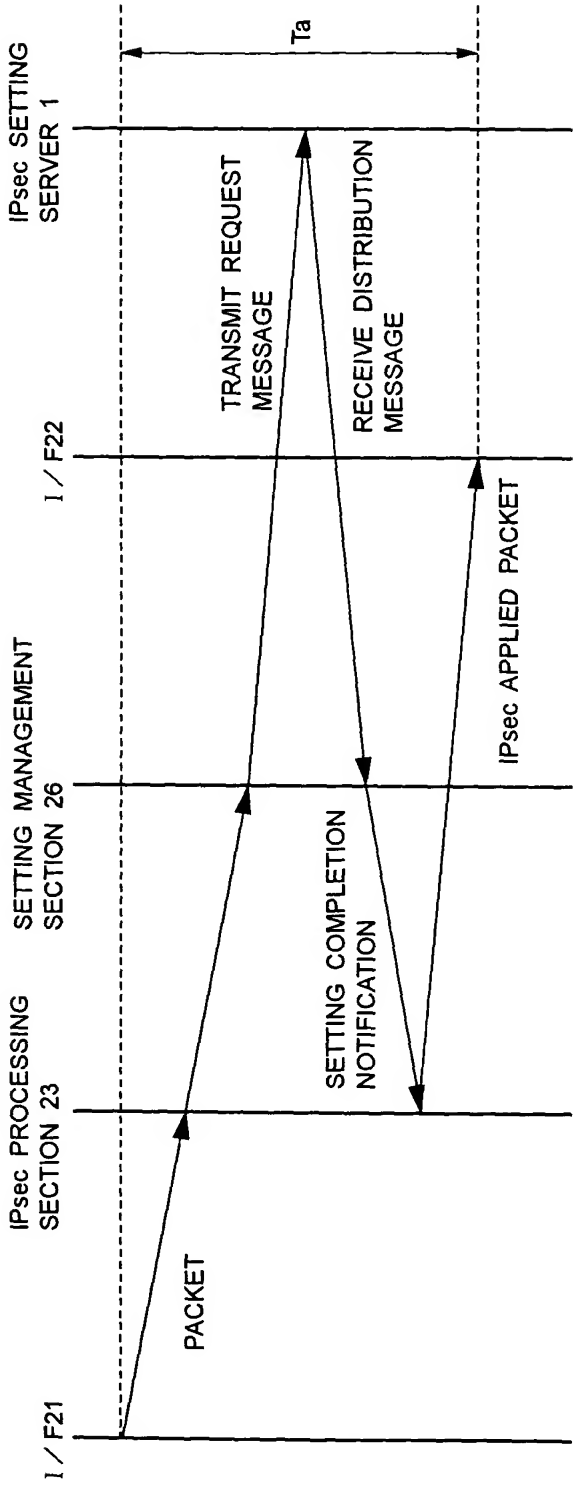
Ta
IPsec SETTING SERVER 1
1 / F22
SETTING MANAGEMENT SECTION 26
IPsec PROCESSING SECTION 23
1 / F21
TRANSMIT REQUEST MESSAGE
RECEIVE DISTRIBUTION MESSAGE
IPsec APPLIED PACKET
SETTING COMPLETION NOTIFICATION
PACKET

FIG. 29

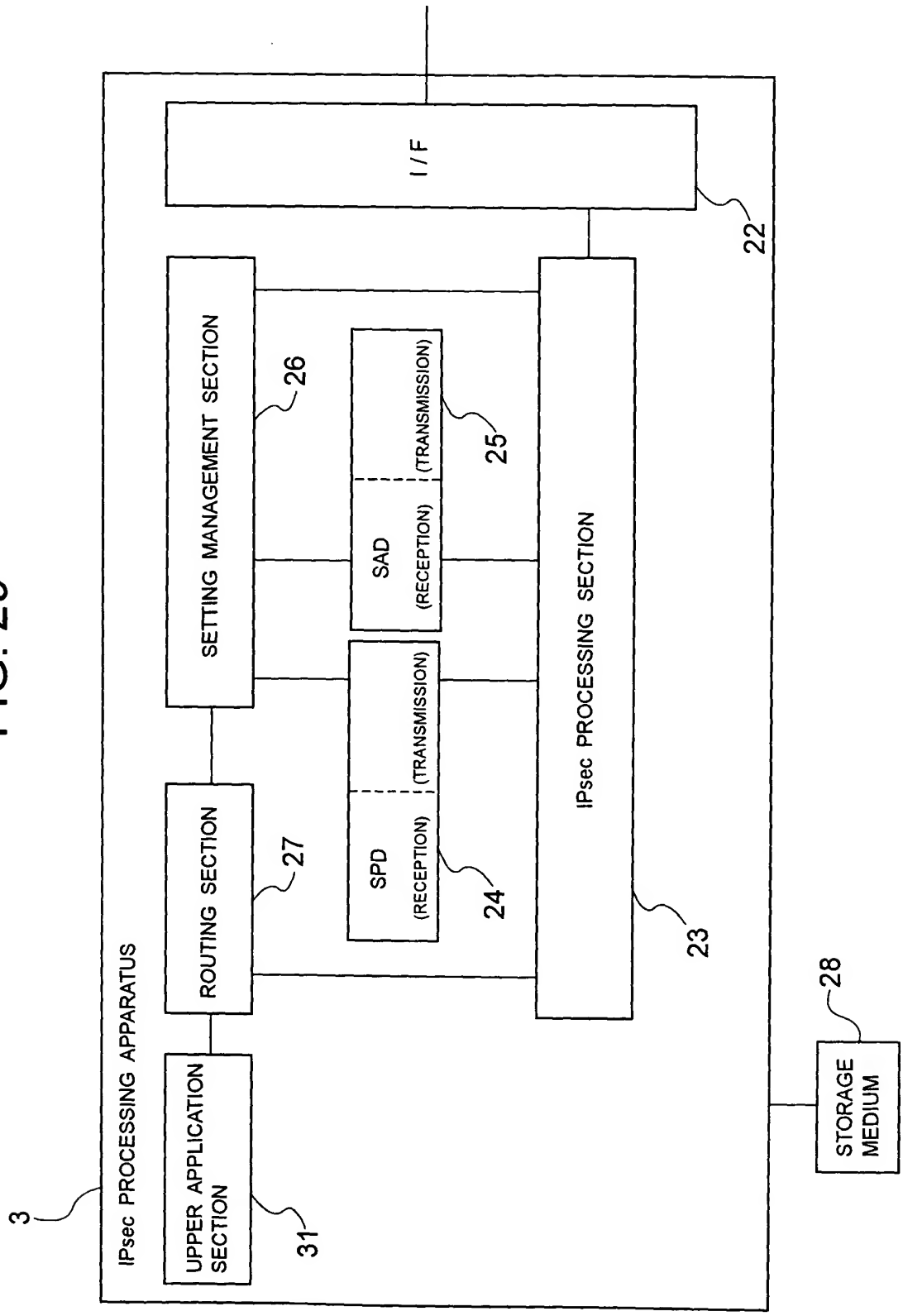
3
IPsec PROCESSING APPARATUS
UPPER APPLICATION SECTION
31
ROUTING SECTION
27
SETTING MANAGEMENT SECTION
26
SPD
(RECEPTION)
(TRANSMISSION)
24
SAD
(RECEPTION)
(TRANSMISSION)
25
IPsec PROCESSING SECTION
23
I / F
22
STORAGE MEDIUM
28

FIG. 30

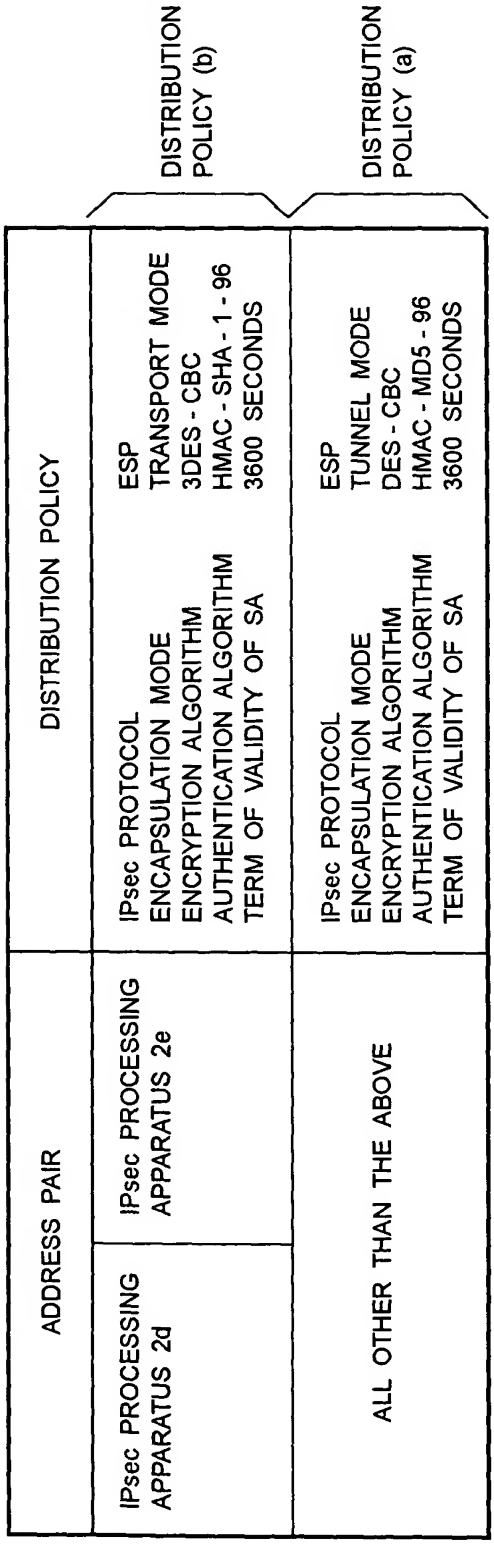
ADDRESS PAIR
DISTRIBUTION POLICY
IPsec PROCESSING APPARATUS 2d
IPsec PROCESSING APPARATUS 2e
ALL OTHER THAN THE ABOVE
IPsec PROTOCOL ESP
ENCAPSULATION MODE TRANSPORT MODE
ENCRYPTION ALGORITHM 3DES - CBC
AUTHENTICATION ALGORITHM HMAC - SHA - 1 - 96
TERM OF VALIDITY OF SA 3600 SECONDS
DISTRIBUTION POLICY (b)
IPsec PROTOCOL ESP
ENCAPSULATION MODE TUNNEL MODE
ENCRYPTION ALGORITHM DES - CBC
AUTHENTICATION ALGORITHM HMAC - MD5 - 96
TERM OF VALIDITY OF SA 3600 SECONDS
DISTRIBUTION POLICY (a)

FIG. 31
PRIOR ART

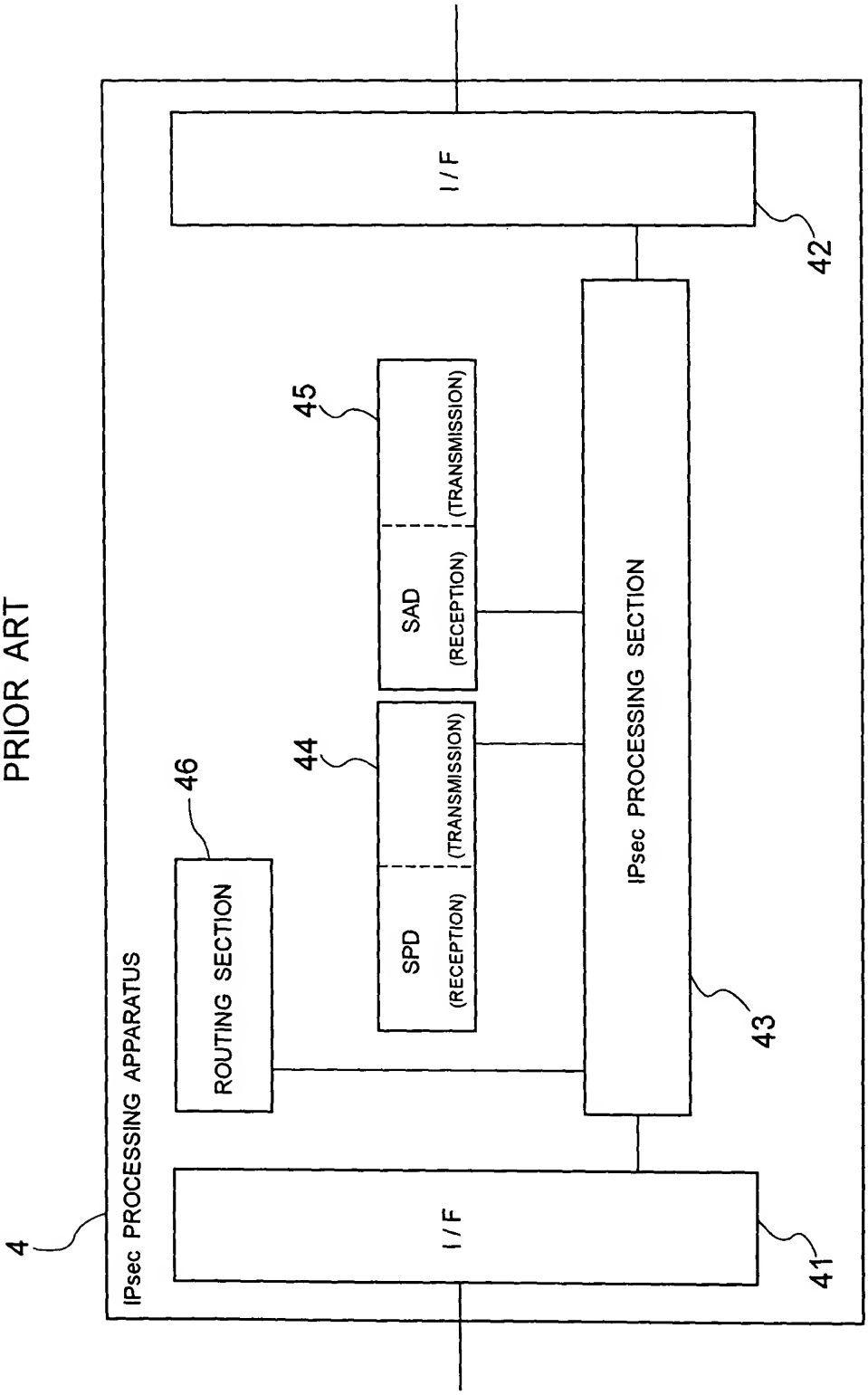

FIG. 32
PRIOR ART

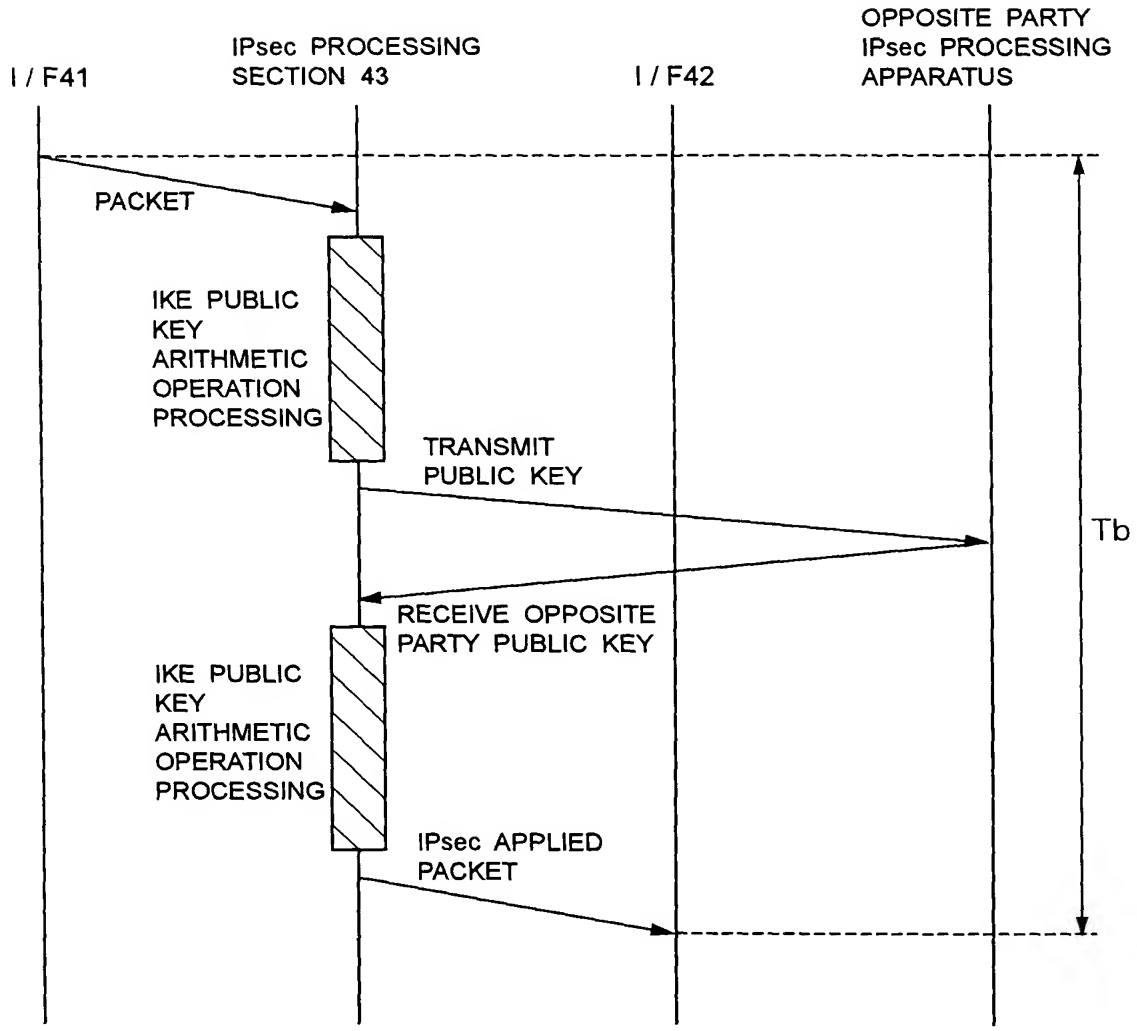

FIG. 33
PRIOR ART